FIG. 1

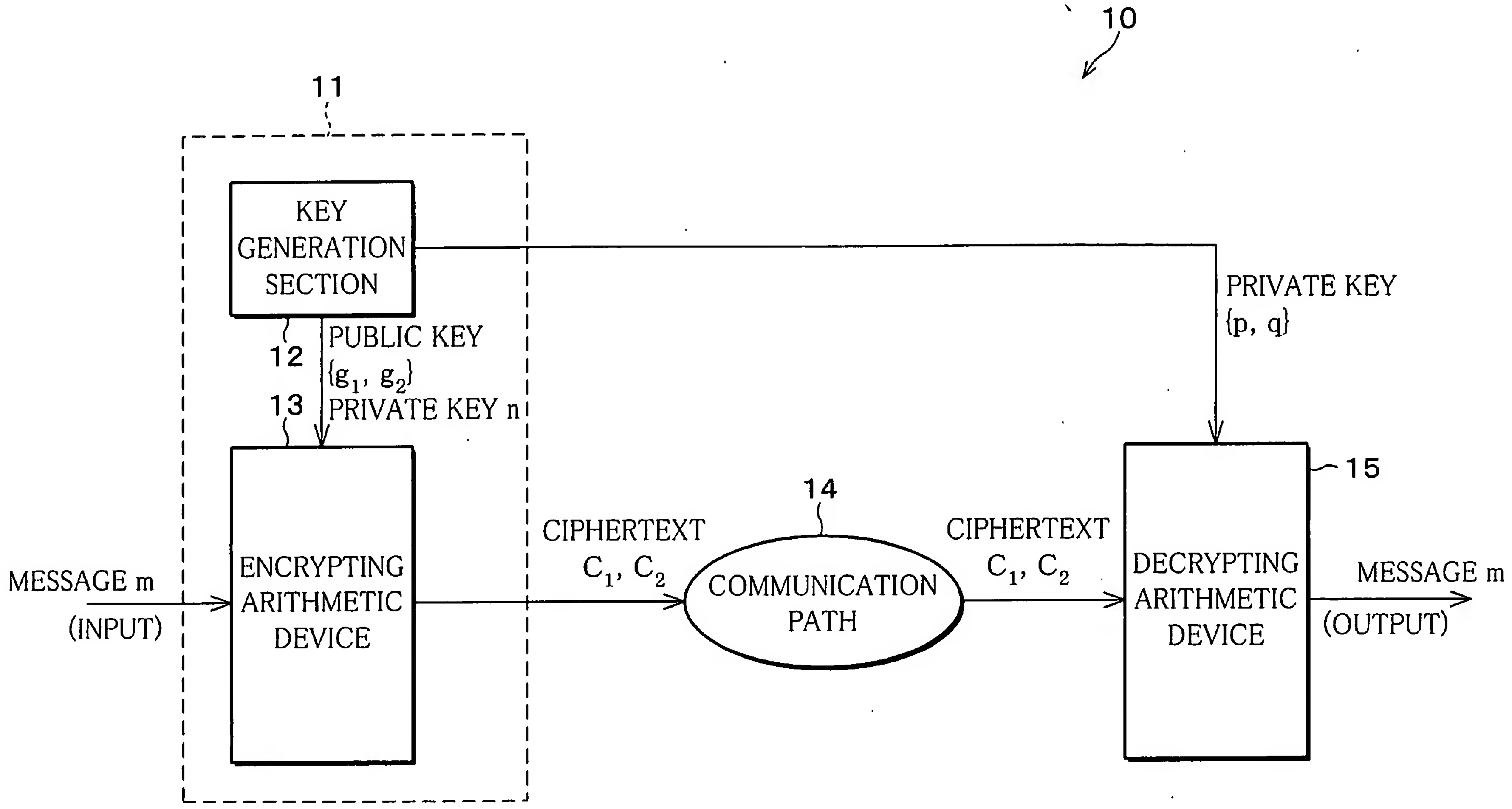

10
11
KEY GENERATION SECTION
12
13
PUBLIC KEY
$\{g_1, g_2\}$
PRIVATE KEY n
MESSAGE m
(INPUT)
ENCRYPTING ARITHMETIC DEVICE
CIPHERTEXT
C_1, C_2
14
COMMUNICATION PATH
CIPHERTEXT
C_1, C_2
PRIVATE KEY
$\{p, q\}$
15
DECRYPTING ARITHMETIC DEVICE
MESSAGE m
(OUTPUT)

FIG. 2

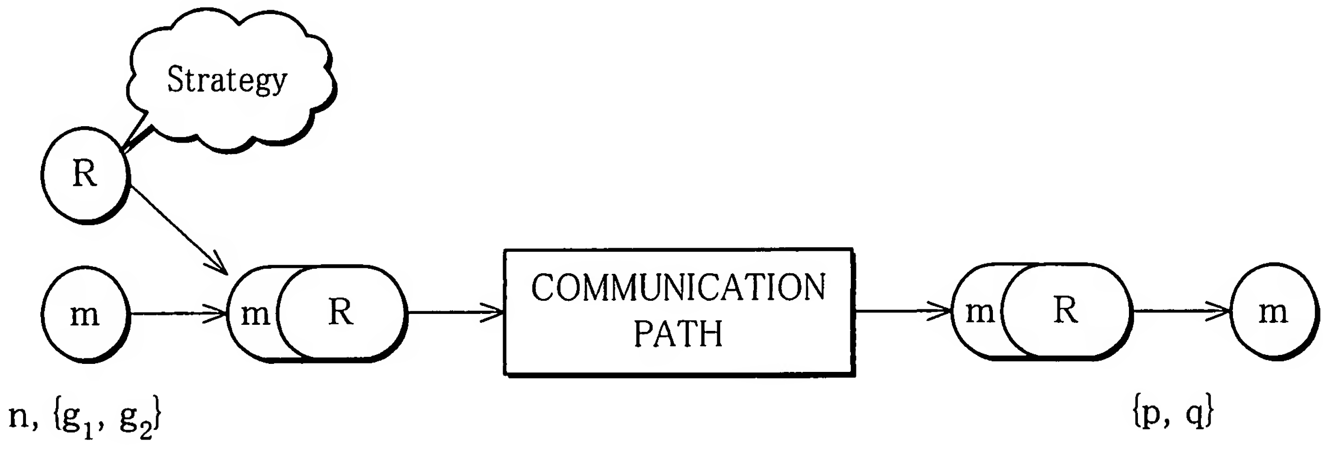
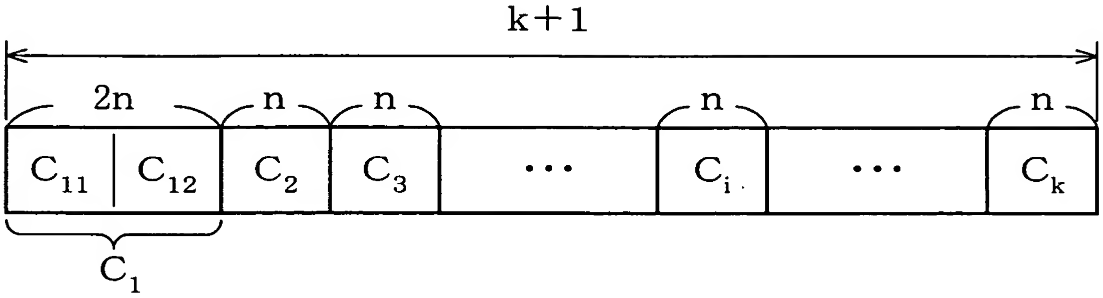


FIG. 3



$$C_1=(C_{11},\ C_{12}),\quad C_{11}=m_1R_1(\mathrm{mod}\ \ n),\quad C_{12}=m_1R_2(\mathrm{mod}\ \ n)$$

$$C_i=m_i\oplus R_{b_i+1};\quad b_i=0\mathrm{or}1\in m_1,\quad 2\le i\le k<\lfloor \log_2 n\rfloor$$